


[Advanced Search](#)
[Preferences](#)
[Language Tools](#)
[Search Tips](#)

[Web](#) - [Images](#) - [Groups](#) - [Directory](#) - [News](#)
Searched the web for **fingerprint consider image**.Results **11 - 20** of about **19,100**. Search took **0.14** second

Looking for pictures? Try Google Image Search by clicking the Images tab.

AST - Fingerprint processing software

... For two different **fingerprint** images, the system calculates a ... an **image** against itself (same **image**), and, on ... value of similitude from which we **consider** that the ...

www.ast-afis.com/uk/uk-Soft.htm - 14k - [Cached](#) - [Similar pages](#)

AutomatedBuildings.com Article - Brilliant Security for ...

... Another impact to **consider** is the decreasing size of the sensor because in ... As sensor size decreases the fraction of the total **fingerprint image** is reduced. ...

www.automatedbuildings.com/news/jun02/art/bioscrypt/bio.htm - 20k - Jul 10, 2003 - [Cached](#) -

[Similar pages](#)

PDF Hiding Fingerprint Minutiae in Images

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... In our application, we **consider** three different types of cover **image** for this purpose: synthetic **fingerprint** images, face images and arbitrary images. ...

biometrics.cse.msu.edu/autoid02-n35-jain-uludag.pdf - [Similar pages](#)

Fingerprint Backgrounder

... (As we **consider** the complexities of ... silicon sensor which is used to capture unique **fingerprint** information. ... plates create an 8-bit (256 gray levels) **image** of a ...

www.veridicom.com/technology/backgrounder.htm - 32k - [Cached](#) - [Similar pages](#)

PDF Fingerprint Minutiae: A Constructive Definition

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... published method of feature extraction (eg, [2]) computes the orientation field of the **fingerprint image**, which reflects ... Now, **consider** an **image** block around ...

www.research.ibm.com/ecvg/pubs/aws-constructive.pdf - [Similar pages](#)

Fingerprint Recognition

... **Image** databases - **fingerprint image** databases, available for testing ... to any other available **fingerprint** search algorithm ... East Shore will **consider** ventures in a ...

www.east-shore.com/over.html - 10k - [Cached](#) - [Similar pages](#)

Identix Inc. - Empowering Identification™ - Understanding ...

... and all other biometrics, there are factors to **consider** when discussing the accuracy of **fingerprint** identification. To obtain a usable **image**, one where the ...

www.identix.com/newsroom/news_biometrics_finger_acc.html - 20k - [Cached](#) - [Similar pages](#)

PS WWW.novodynamics.com/trenkle/papers/aipr93.ps.gz

File Format: Adobe PostScript - [View as Text](#)

... which a classification algorithm must **consider** by determining ... of interest (ROIs) for classifying **fingerprint** images ... to locate regions in the **image** which contain ...

[Similar pages](#)

Latent Print Examination

... **Image** of a spinning world, Please click here to participate in the IAI AFIS survey. ... If you are a **Fingerprint** Professional, you should **consider** joining the ...

Description: Information about finger and palmprint examination, the processing of latent prints, and links.

Category: [Science > Science in Society > Forensic Science > Fingerprints](#)

onin.com/fp/ - 90k - Jul 10, 2003 - [Cached](#) - [Similar pages](#)

Sponsored Links

All About Fingerprints

Standalone OEM module, Algorithm Support various fingerprint sensor
www.suprema.co.kr

Interest: [View details](#)

Fingerprint Development

Labcaire's new fully automated fingerprint development cabinet
www.labcaire.co.uk

Interest: [View details](#)

FBI Results. Fast

FBI Fingerprint Card Scanning - A Results in Days instead of months
www.FBIfingerprints.com

Interest: [View details](#)

Biometric Fingerprints

Fingerprint Biometric Guide, find Vendors, Articles & News.

www.findbiometrics.com

Interest: [View details](#)

Fingerprint Search Engine

FP-Sensor independent Win SDK for exact high speed recognition
www.biometrix.at

Interest: [View details](#)

[See your message here.](#)

新網頁 1

... test neighbors, we give the test **fingerprint** "1" point ... test center extremely well,
the test **image** can score ... the one used in warping), we **consider** the reference ...

ise0.stanford.edu/class/ee368a_proj01/ dropbox/project22/finger/veri.htm - 12k - [Cached](#) - [Similar pages](#)

◀ Goooooooooooooogle ▶

Result Page: [Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [Next](#)

fingerprint consider image

Google Search

[Search within results](#)

[Google Home](#) - [Advertise with Us](#) - [Business Solutions](#) - [Services & Tools](#) - [Jobs, Press, & Help](#)

©2003 Google

L Number	Hits	Search Text	DB	Time stamp
1	277	biometric\$6 with image\$6	USPAT	2003/07/11 10:51
2	32	biometric\$6 with measure\$6 with image\$6	USPAT	2003/07/11 10:42
3	95	(biometric\$6 with image\$6) and (7\$/\$).ccls.	USPAT	2003/07/11 11:09
4	0	(visage near development).as.	USPAT	2003/07/11 11:09
5	3	(visage).as.	USPAT	2003/07/11 11:10
6	9	(ryan near andrew).in.	USPAT	2003/07/11 11:11
7	0	5280527.pn. and (image\$5)	USPAT	2003/07/11 12:18
8	1	5280527.pn. and (stor\$6 same (finger\$6 sample\$5))	USPAT	2003/07/11 12:29
13	19	(biometric adj sensor\$4) with image\$5	USPAT	2003/07/11 13:05
14	21	(biometric\$5 near sensor\$4) with image\$5	USPAT	2003/07/11 14:12
15	1	5280527.pn. and (face\$3 facial\$5 fingerprint\$5)	USPAT	2003/07/11 14:15

This is Google's cache of <http://www.informationweek.com/644/44iubod.htm>.

Google's cache is the snapshot that we took of the page as we crawled the web.

The page may have changed since that time. Click here for the [current page](#) without highlighting.

To link to or bookmark this page, use the following url: [http://www.google.com/search?](http://www.google.com/search?q=cache:L8gDa8uMf84J:www.informationweek.com/644/44iubod.htm+biometrics+++digitize+digital&hl=en&ie=UTF-8)

[q=cache:L8gDa8uMf84J:www.informationweek.com/644/44iubod.htm+biometrics+++digitize+digital&hl=en&ie=UTF-8](http://www.google.com/search?q=cache:L8gDa8uMf84J:www.informationweek.com/644/44iubod.htm+biometrics+++digitize+digital&hl=en&ie=UTF-8)

Google is not affiliated with the authors of this page nor responsible for its content.

These search terms have been highlighted: **biometrics digitize digital**

NEW

EVENT

LISTENING POST

RESEARCH REPORT

SUBSCRIPTION

Part of the **TechWeb** Business Technology Network

InformationWeek
United Business Media BUSINESS INNOVATION POWERED BY TECHNOLOGY

Giving Grids A Go
Hewitt Associates is a grid-computing convert

Tech Guide
Standards, cheap hardware make going wireless easier

SEARCH SITE

> HARDWARE > SOFTWARE > SECURITY > INDUSTRIES > BUSINESS SERVICES > CAREER DEVELOPMENT

INFORMATIONWEEK ONLINE NEWS IN REVIEW

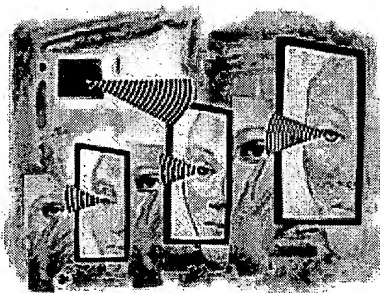
August 18, 1997

Body Language

Fingerprints, faces, even eyes are the new keys to protecting secure systems

By [Bob Violino](#)

Your fingerprints are unique. So is your voice, your face, even the iris of your eye. And all these unique parts of your body can function as keys that unlock IT security systems. Welcome to the world of **biometrics**: the science of using **digital** technology to identify individuals based on their physical characteristics.



For years, the only users of **biometrics** for security have been the military, law enforcement organizations, a few government agencies-and characters in Hollywood movies. Businesses have largely ignored the technology, either because they found it was too expensive or because they simply didn't know much about it.

All that's changing. The prices of biometric products are falling as new vendors jump into the market. Businesses-led by banks and other financial services companies concerned about rising information-security threats-view **biometrics** as both a potential replacement for passwords and a major component of their security strategy. The key word is potential. More product testing is probably needed, and prices may need to drop further before **biometrics** go mainstream.

Biometrics could be the best way to authenticate users. It's been used primarily for physical access-for example, fingerprint readers that control the door to a restricted room. **Biometrics** vendors are developing new products for computer and network access, too. "The future is **biometrics**," says Joel Lisker, a former FBI agent who is now senior VP of security and risk management at MasterCard International Inc. MasterCard is testing a system that uses fingerprint components for identification. It has also explored voice-recognition, face-recognition, and iris-scanning security systems.



Man of vision: "The future is biometrics," says MasterCard International's senior VP Lisker

Lisker's opinion aside, **biometrics** systems are still largely unused and unknown among IS managers in business. In an InformationWeek survey of 134 IS managers, conducted early this summer, only 4% of respondents reported using biometric technology in their organizations. When asked to identify the technology's biggest drawbacks, about half the overall group cited their own lack of knowledge about the technology. Nearly one-third complained of high costs.

IT managers who are aware of the technology are embracing it. At MasterCard, Lisker is testing a fingerprint system from Identicator Technology Corp. of San Bruno, Calif., that will control visitors' access to the credit-card company's headquarters in Purchase, N.Y. The pilot program, which began a year ago, will soon expand to incorporate the use of smart cards that store fingerprint data.

MasterCard plans to test the fingerprint system for identifying credit-card holders during transactions. The company thinks it could also be used to control employee access to desktop and portable computers and networks. "It has been extraordinarily reliable," Lisker says. "The technology is far more robust than it was two years ago-and I thought it was impressive then."

Fingerprints Are First

In fact, many say fingerprint-ID technology is the most advanced of the **biometrics**, and the most likely to make a splash in the business market. For one, these systems are reasonably easy to use and relatively nonintrusive. For another, vendors of fingerprint systems can draw on years of experience that have already gone into automated fingerprint-ID systems widely used by law-enforcement agencies and the government.

For example, Connecticut's Department of Social Services in Hartford has used fingerprint identification in its statewide welfare benefits program since January 1996. The three-year, \$5.1 million project, in which welfare recipients use a fingerprint-ID system when picking up their checks, has saved the state \$9 million by catching welfare cheats, says David Mintie, director of the **Digital Imaging Project**, Connecticut's fingerprint-scanning initiative.

The system uses a **digital** camera to capture images of fingerprints, then stores them on servers equipped with imaging software from National Registry Inc. Recipients who claim checks in person must place their finger in a scanner at the regional welfare office to verify their identity. The scanners, from Identix Corp. of Sunnyvale, Calif., cost \$200 each. The department also uses the fingerprint system for PC access on 77 desktops, and it plans to expand to more desks when scanner prices drop. **Biometrics** prices "change radically every six months," Mintie says.

Fingerprint systems are already making their way into data centers. Database vendor Oracle, among others, expects fingerprint-ID systems to be broadly accepted. The Redwood City, Calif., company recently began shipping a version of its Oracle7 database equipped with a fingerprint-ID security system. Through an agreement, Oracle provides Identix's Touchnet II, which consists of a scanner, PC Card, and software as part of Oracle7's advanced networking option. Oracle will offer similar features in other products, including the recently unveiled Oracle8 database. "Fingerprint authentication is one of the most mature **biometrics**," says Wynn White, director of middleware product management at Oracle.

Fingerprint **biometrics** got a huge boost in May, when Veridicom Inc., a Menlo Park, Calif., startup formed by Lucent Technologies and U.S. Venture Partners, announced the development of a stamp-sized fingerprint reader. The reader-on-a-chip, which is smaller than optical fingerprint readers, can be built into a computer keyboard or mouse, allowing verified users to gain access to a PC or notebook. The chip has thousands of built-in sensors that bounce minute electrical charges off a user's skin, which measure the ridges of the fingerprint.

Accompanying software products reconstruct the fingerprint in **digital** form, search for unique features, and use special algorithms to match the print to a sample given earlier by the user.

When a user wants to access the device, he or she places a finger on the chip and the software verifies a match. Additional software protects prints from unauthorized copying or tampering, and Veridicom says the sensor can be used with other security measures such as public and private keys and **digital** signatures. The system, including the chip and software, will begin shipping by the end of the year for about \$300. Tom Rowley, Veridicom's CEO, predicts the cost will eventually drop to as low as \$100.

Veridicom says several computer makers intend to use the chip, but has so far declined to name names.

Miniaturized systems like Veridicom's will likely help spur demand. "We're beginning to see a lot of interest in fingerprint technology, especially with the prospect of building scanners into a keyboard or mouse for remote network access," says Jackie Fenn, VP and research director for advanced technologies at Gartner Group Inc., an IT advisory firm in Stamford, Conn.

Still, Fenn notes that since these features will add several hundred dollars to the cost of desktop devices, she doesn't expect widespread use of built-in scanners until unit prices drop below \$200.

Surge From Falling Prices

As those prices fall, companies should expect to see the emergence of some type of fingerprint-ID feature on high-end notebooks by the middle of next year, says Chris Byrnes, VP for services and systems management strategy at Meta Group in Reston, Va. With the Veridicom chip comes "the first technology for taking fingerprint identification and building it into a PC," adds Byrnes.

Optical fingerprint systems are also finding their way into desktop PCs and notebooks. Identicator, for one, is talking to several major computer, mouse, and keyboard makers about incorporating its system into their products. Identicator's president, Oscar Pieper, expects to see PCs equipped with fingerprint-ID systems by year's end. He says the security feature will add about \$100 to these devices' prices when purchased in large volumes.

Fingerprint-ID products will need to interoperate, too, say industry sources. "To have any kind of mass implementation, we're going to have to have the ability for all readers to read certain patterns," says Ann Brown, VP of U.S. operations at

Mytec Technologies Inc. in Toronto, which makes a \$995 fingerprint-ID system that includes data encryption software to ensure safer transmission of fingerprint data over the Internet.

Another type of biometric security system-iris scanning-is being tested, too. Citicorp in New York is testing an iris-scanning system from Sensar Inc. of Moorestown, N.J., and is looking into other types of biometric technology. Jim Zeanah, chief technology officer for Citicorp's development division, calls iris-scanning technology impressive, though not quite ready for industrial-strength production. "We consider this an early investment in a technology that has a lot of potential," he says.

Citicorp has also investigated voice-verification, voice-authentication, and fingerprint scanning, but finds iris technology to be the most accurate way to identify people. "Ninety-five percent isn't good enough," Zeanah says. "It needs to be well above 99%." Zeanah believes iris scanning has the highest potential to reach that.

No Two The Same

IriScan Inc. in Mount Laurel, N.J., which holds exclusive patents for iris-recognition hardware and software, says the technology is reliable because, in the entire human race, no two irises have the same detail, not even among identical twins. Fingerprints, however, have 60 different variations from which to compare and analyze, making identification less reliable, says Kelly Gates, marketing manager at IriScan.

Iris scanners take a high-resolution picture of a person's iris, **digitize** the image, and store the data in a database on a server or host system. Then, each time a person wants access to a device, he or she must look into a camera and wait for the system to determine that the iris' pattern matches the image in the file.

There are a few barriers. For one, not everyone likes using iris-scanning products. Some users fear the systems will damage their eyes. But vendors insist the systems use ordinary cameras and lights and are safe.

Also, iris scanners are costly. Sensar's IrisIdent, for example, costs about \$6,500. That includes an optical camera and processing platform, Pentium processor, and software. Yet Sensar's president and CEO, Thomas Drury, says the product's ease of use and reliability make up for the high cost.

Drury expects price to become less of a factor as companies leverage investments they're already making in videoconferencing cameras, since the iris systems use standard video cameras. If a company already has the cameras in place, it's likely to be more interested in buying the

other equipment needed to round out a complete system. Drury also predicts that lower-cost iris systems for desktop use-how low, he won't say-are about 18 months away.

Voice verification is another biometric technology that's catching on as a viable security alternative. Chase Manhattan Corp. in New York has tested voice-verification technology with 9,000 employees in many of its bank branches. The bank is also participating in a fingerprint trial at the U.S. National Biometric Test Center at San Jose State University (Chase is evaluating iris scanning there as well).

Chase, like many other companies, is waiting for prices to drop before it adopts **biometrics** on a wide scale. If and when prices do drop, the bank expects to use **biometrics** in conjunction with personal ID numbers and passwords for access to company computers and networks. "Some products have the potential for being cost-effective," says Adam Backenroth, VP of corporate emerging technologies at Chase.

An Ear For Security

Judith Markowitz, an independent consultant in speech and voice verification in Chicago, says one advantage of voice-verification technology is its use of ordinary phones. That helps eliminate the need for special equipment or training.

That benefit is helping Glenview State Bank, which is using voice verification and recognition to boost customer service. Its system, from Intervoice in Dallas, lets customers retrieve balance information and transfer funds via telephone. Statistics gathered over the first year of the trial show that customers use it every hour of the day. "It's been very accurate; we've had no problems," says Betsy Wexler, VP of operations of Glenview in Glenview, Ill. "The customers appreciate that we're doing it."

Another biometric technology that shows potential is face recognition. Among its proponents: Mr. Payroll Corp., a unit of Cash America International in Fort Worth, Texas. The check-cashing services provider is using a product called TrueFace from Miros Inc. in Wellesley, Mass., to identify customers at check-cashing machines. While Mr. Payroll's is a narrow application, the company believes face recognition could be used for access to PCs. "It's a very good application for PCs," says Mike Stinson, president of Mr. Payroll. "If it will work in the retail environment, with thousands of people a day, it will certainly work in the office environment."

Miros technology compares an image from a standard security camera with the stored images of authorized users in less than a second. Users first submit to a brief video scan, during which an image of their face is recorded, then digitized and stored on a database. Once that's done, the face-

recognition system is easy to use. "There's nothing to touch," says Miros founder and CEO Michael Kuperstein. "The more you minimize the burden, the more people will accept it."

Another supplier of face-recognition technology, Visionics Corp. in Metuchen, N.J., introduced a \$300 system in April. The company's Facelt PC 2.5 includes a video camera, video board, and face-recognition software, and it runs on Windows NT and Windows 95 PCs. Joseph Atick, president of Visionics, admits that use of face recognition for corporate IT security applications has been only "sporadic," but he expects the market to grow as computer manufacturers incorporate face identification in their systems.

How big is the market for **biometrics** devices? It depends on whom you ask. Erik Bowman, an analyst for Personal Identification News, a monthly newsletter that tracks the biometric industry, predicts an annual growth rate of 27% to 35% through 2000. He says demand for **biometrics** will be driven by the growth of electronic commerce and intranets, and sales will be boosted by shrinking product size and greater awareness. Similarly, Infosecurity News, a monthly publication covering the information security business, in its annual industry survey in May cited **biometrics** as the fastest-growing product category.

Others are skeptical about the near-term viability of **biometrics** for corporate security applications. "I don't see this as a realistic solution for general business for a long time to come," says Richard Power, senior consultant at Computer Security Institute, a San Francisco group that represents IT security chiefs.

Power says that even with costs coming down, **biometrics** devices will continue to cost more than other security options. "This is especially true when you're talking about enterprisewide networks with hundreds of thousands of users, wire- less systems, notebooks, telecommuters," he adds. Power also questions whether less costly systems will be reliable enough. "There's always the possibility of technological breakthroughs," he says, "but I don't see it happening."

Still others see **biometrics** playing a niche role in info security. Handwriting recognition, for example, could be practical for access to personal **digital** assistants that have pen input devices, suggests Ken Cutler, director of information security at the MIS Training Institute in Framingham, Mass.

Many in the security industry see the need for **biometrics** standards. That would help guide product development and assure that systems from different vendors work together. Standards efforts are under way. At the BiometricCon '97

conference earlier this year, a group of companies led by Novell announced the Speaker Verification Application Programming Interface Standard (SVAPI), which sets APIs for developers building speaker-verification technology into desktop and network applications. The standard allows interoperability over distributed environments with related APIs, including Microsoft's SAPI, a proprietary API for Windows 95 and Windows NT; the telecom industry's S100 architecture for developing computer-telephony applications; and Sun Microsystems' JavaSpeech speech-recognition standard.

The first SVAPI-compliant products will appear in the third quarter, predicts Bruce Armstrong, manager of speech technologies at Novell and chairman of the SVAPI work group (other members include Citicorp, IBM, Texas Instruments, the Internal Revenue Service, and the Department of Defense). For example, Novell is testing prototypes that could let users log onto a NetWare network after first passing a voice-verification test, Armstrong says.

Also, some industry observers are calling for additional independent testing of all types of products. "It's amazing how little is known about this," says Jim Wayman, a **biometrics** scientist and director of biometric research at the National Biometric Test Center in San Jose, Calif.

Wayman and his colleagues are trying to rectify that. The National Biometric Test Center started work in April after receiving a \$1.6 million grant from the Department of Defense. It tests biometric products and reports its findings to the department. Many security managers, hoping to gain new weapons to fight off threats to information security, will be eager to see the results.

► [Back to News in Review](#)

► [Send Us Your Feedback](#)

► [Top of the Page](#)



